FIPS 140-2 Nonproprietary Security Policy: Nokia IP350 and IP380 Security Platforms

Hardware Versions: NBB335F000 (IP350), NBB335FFRU (IP350), NBB338F000 (IP380), and NBB338FFRU (IP380)

Software Versions: IPSO v3.7.99 and Check Point VPN-1 NG with Application Intelligence Release 54

Level 2 Validation
Version 1.01

Part No. N451316004 Rev A

Published June 2004

COPYRIGHT

RESTRICTED RIGHTS LEGEND

Use, duplication, or disclosure by the United States Government is subject to restrictions as set forth in subparagraph (c)(1)(ii) of the Rights in Technical Data and Computer Software clause at DFARS 252.227-7013.

Notwithstanding any other license agreement that may pertain to, or accompany the delivery of, this computer software, the rights of the United States Government regarding its use, reproduction, and disclosure are as set forth in the Commercial Computer Software-Restricted Rights clause at FAR 52.227-19.

IMPORTANT NOTE TO USERS

This software and hardware is provided by Nokia Inc. as is and any express or implied warranties, including, but not limited to, implied warranties of merchantability and fitness for a particular purpose are disclaimed. In no event shall Nokia, or its affiliates, subsidiaries or suppliers be liable for any direct, indirect, incidental, special, exemplary, or consequential damages (including, but not limited to, procurement of substitute goods or services; loss of use, data, or profits; or business interruption) however caused and on any theory of liability, whether in contract, strict liability, or tort (including negligence or otherwise) arising in any way out of the use of this software, even if advised of the possibility of such damage.

Nokia reserves the right to make changes without further notice to any products herein.

TRADEMARKS

Nokia is a registered trademark of Nokia Corporation. Other products mentioned in this document are trademarks or registered trademarks of their respective holders.

040113

Nokia Contact Information

Corporate Headquarters

Web Site	http://www.nokia.com
Telephone	1-888-477-4566 *or* 1-650-625-2000
Fax	1-650-691-2170
Mail Address	Nokia Inc. 313 Fairchild Drive Mountain View, California 94043-2215 USA

Regional Contact Information

Americas	Nokia Inc. 313 Fairchild Drive Mountain View, CA 94043-2215 USA	Tel: 1-877-997-9199 Outside USA and Canada: +1 512-437-7089 email: ipsecurity.na@nokia.com
Europe, Middle East, and Africa	Nokia House, Summit Avenue Southwood, Farnborough Hampshire GU14 ONG UK	Tel: UK: +44 161 601 8908 Tel: France: +33 170 708 166 email: ipsecurity.emea@nokia.com
Asia-Pacific	438B Alexandra Road #07-00 Alexandra Technopark Singapore 119968	Tel: +65 6588 3364 email: ipsecurity.apac@nokia.com

Nokia Customer Support

Web Site:	https://support.nokia.com/		
Email:	tac.support@nokia.com		
Americas		**Europe**	
Voice:	1-888-361-5030 or 1-613-271-6721	**Voice:**	+44 (0) 125-286-8900
Fax:	1-613-271-8782	**Fax:**	+44 (0) 125-286-5666
Asia-Pacific			
Voice:	+65-67232999		
Fax:	+65-67232897		

031014

Contents

Preface

Purpose

This document is a nonproprietary Cryptographic Module Security Policy for the Nokia IP350 and IP380 appliances. This security policy describes how the IP350 and IP380 meet the security requirements of FIPS 140-2 and how to run the modules in a secure FIPS 140-2 mode. This policy was prepared as part of the Level 2 FIPS 140-2 validation of the module.

The FIPS 140-2 (Federal Information Processing Standards Publication 140-2—*Security Requirements for Cryptographic Modules*) details the U.S. Government requirements for cryptographic modules. More information about the FIPS 140-2 standard and validation program is available on the National Institute of Standards and Technology (NIST) Cryptographic Module Validation Program (CMVP) Web site at http://csrc.nist.gov/cryptval/.

The Nokia IP350 and IP380 appliances are referred to in this document as IP security platforms, security platforms, platforms, and the modules. The differences between the modules are pointed out where appropriate.

References

This document deals only with operations and capabilities of the module in the technical terms of a FIPS 140-2 cryptographic module security policy. More information is available on the module from the following sources:

- The Nokia Web site (http://www.nokia.com/) contains information on the full line of products from Nokia.
- The CMVP Web site (http://csrc.nist.gov/cryptval/) contains contact information for answers to technical or sales-related questions for the module.

FIPS 140-2 Submission Package Documents

The security policy document is one document in a FIPS 140-2 Submission Package. In addition to this document, the submission package contains:

- Vendor Evidence document
- Finite State Machine
- Other supporting documentation as additional references

This security policy and the other validation submission documentation were produced by Corsec Security, Inc. under contract to Nokia. With the exception of this nonproprietary security policy, the FIPS 140-2 validation documentation is proprietary to Nokia and is releasable only under appropriate nondisclosure agreements. For access to these documents, contact Nokia.

1 Nokia IP350 and IP380 Security Platforms

Overview

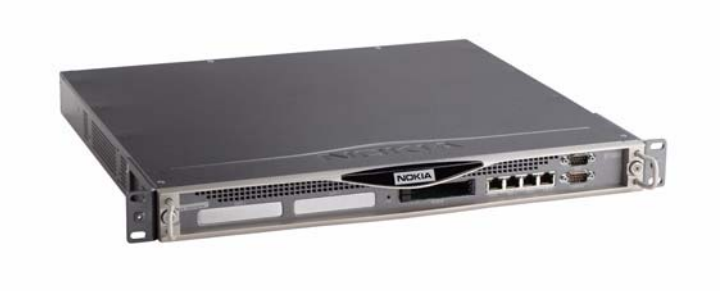
The *New Look and Feel* Nokia IP350 and IP380 are IP security platforms designed to provide a secure, reliable, and manageable integrated security solution for secure Internet communication and access control for networks. The security platforms combine the security-hardened operating system, IPSO, with the market-leading Check Point FireWall-1 (FW-1) and VPN-1 Next Generation (NG) suite software on a purpose-built security hardware platform. As network devices, the Nokia IP350 and IP380 support a comprehensive suite of IP-routing functions and protocols, including RIPv1/RIPv2, IGRP, OSPF and BGP4 for unicast traffic, and DVMRP for multicast traffic.

Some highlighted security features of the IP350 and IP380 appliances are:

- Read/write and read-only access modes
- Screening of all incoming communications to ensure authorized user access
- SSH-secured remote management of the modules (Nokia IPSO)
- SSHv1 and SSHv2 supported
- TLS-secured remote management of Check Point applications
- Secure VPN between subsystems
- Multiple layers of authentication required when accessing the remote management interface for IPSO

Both platforms share the same one-rack unit size and include serviceability features such as a slide-out access tray for quick and easy installation of cards or memory without having to unrack the unit. The IP350 and IP380 have the connectivity flexibility a network needs with four integrated and fully routable Ethernet ports and two option slots supporting either WAN cards or dual-port Ethernet cards for up to eight 10/100 ports.

Figure 1 Nokia IP380 appliance



The Nokia IP350 and IP380 are differentiated through their performance levels. The IP350 reaches 350 Mbps of secured large packet firewall throughput with high-speed, small-packet performance designed to efficiently support real-world mixed traffic solutions. As a VPN platform, the IP350 encrypts a 3DES VPN at 80 Mbps with on-board encryption acceleration. The IP380 reaches speeds of 600 Mbps of secured large packet firewall throughput, and encrypts 3DES VPN at almost 90 Mbps or at 130 Mbps with the optional encryption accelerator (this is available only for the IP380). Both platforms greatly accelerate their FireWall-1 performance by using Nokia Firewall Flows.

Cryptographic Module

The Nokia IP350 and IP380 appliances were tested as multichip standalone cryptographic modules. The metal enclosure physically encloses the complete set of hardware and software components, and represents the cryptographic boundary of each module. The security platforms run the security hardened operating system IPSO v3.7.99 and Check Point VPN-1 NG with Application Intelligence R54 software for VPN and firewall functionalities.

The modules are intended to meet overall FIPS 140-2 Level 2 requirements (see Table 1).

Table 1 Intended Level Per FIPS 140-2 Section

Section	Section title	Level
1	Cryptographic Module Specification	2
2	Cryptographic Module Ports and Interfaces	2
3	Roles, Services, and Authentication	2
4	Finite State Model	2
5	Physical Security	2
6	Operational Environment	N/A
7	Cryptographic Key Management	2
8	EMI/EMC	2

Table 1 Intended Level Per FIPS 140-2 Section (*continued*)

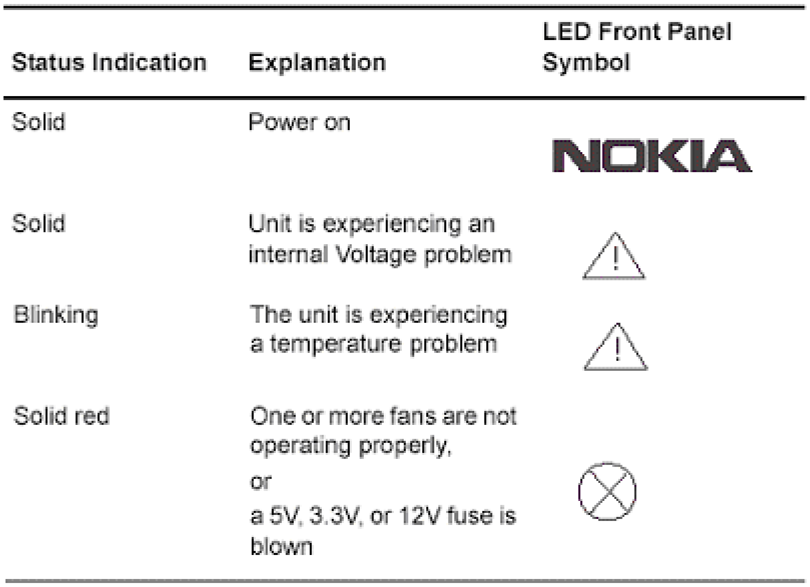
Section	Section title	Level
9	Self-tests	2
10	Design Assurance	2
11	Mitigation of Other Attacks	N/A

Module Interfaces

The security platforms provide a number of physical ports:

- Four Ethernet ports labeled ETH-1, ETH-2, ETH-3, and ETH-4. Each port has two LEDs that indicate port status:
  - Green LED: lights up to indicate a connection
  - Yellow LED: lights up when data is transmitted
- Console port
- AUX port (disabled by default; must not be enabled in FIPS mode)
- Two interface option slots for the following network interface cards:
  - Dual-port 10/100 Ethernet
  - Single-port V.35 or X.21
- Two type II PCMCIA slots (disabled in FIPS mode)
- Power switch
- Power plug
- Reset switch
- Three system status LEDs

The following table shows the system status LEDs and describes their meaning.



Status Indication	Explanation	LED Front Panel Symbol
Solid	Power on	NOKIA
Solid	Unit is experiencing an internal Voltage problem	⚠
Blinking	The unit is experiencing a temperature problem	⚠
Solid red	One or more fans are not operating properly, or a 5V, 3.3V, or 12V fuse is blown	⊗

All of these physical ports are separated into logical interfaces defined by FIPS 140-2, as described in Table 2.

Table 2 FIPS 140-2 Logical Interfaces

Module physical port	FIPS 140-2 logical interface
Network ports	Data input interface
Network ports	Data output interface
Network ports, console port, power switch, reset switch	Control input interface
Network ports, console port, LEDs	Status output interface
Power plug	Power interface

Data input and output, control input, and status output are defined as follows:

- Data input and output are the packets that use the firewall, VPN, and routing functionalities of the modules.
- Control input consists of manual control inputs for power and reset through the power and reset switch. It also consists of all of the data that is entered into the module while using the management interfaces.
- Status output consists of the status indicators displayed through the LEDs and the status data that is output from the modules while using the management interfaces.

The modules distinguish between different forms of data, control, and status traffic over the network ports by analyzing the packets header information and contents.

Roles and Services

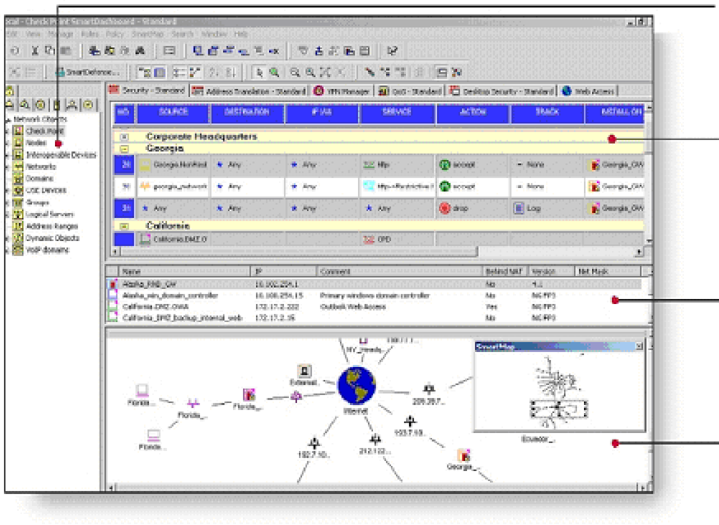
The modules support role-based authentication. The two main roles in the modules (as required by FIPS 140-2) that operators can assume are: a Crypto Officer role and a User role.

Crypto Officer Role

The Crypto Officer role can configure, manage, and monitor the module. Three management interfaces can be used for this purpose:

- CLI–the Crypto Officer can use the CLI to configure and monitor IPSO systems. This can be done locally by using the console port or remotely by using the SSH secured management session.
- SNMP–the Crypto Officer can use SNMPv3 to view MIB values.
- SmartDashBoard–the Check Point TLS-secured Web-based management interface. The Crypto Officer can use this interface after the initial configuration of the Check Point module through the CLI (see Figure 2 on page 13).

Figure 2 Easy to Use Check Point Management Tools



Objects tree contains all objects — for users, hosts, networks and more

Rule base manages Firewall, NAT, QoS, Desktop Security and Web Access policies

Objects list provides easy access to the most commonly used objects

Optional SmartMap module provides a detailed, graphical map of the security

Descriptions of the services available to the Crypto Officer role are provided in Table 3.

Table 3 Crypto Officer Services, Descriptions, Inputs, and Outputs

Service	Description	Input	Output	Critical Security Parameter (CSP) access
Startup configuration	Provide network connectivity and set a password for the admin account	Commands and configuration data	Status of commands and configuration data	Admin password (read/write access)
SSH	Provide authenticated and encrypted sessions while using the CLI	SSH key transport (SSHv1) or SSH key agreement (SSHv2) parameters, SSH inputs, and data	SSH outputs and data	RSA (SSHv1) or DSA (SSHv2) host key pair (read access); RSA (SSHv1) or DSA (SSHv2) authorized key (read access); RSA (SSHv1) or DSA (SSHv2) user key pair (read access); RSA server key (SSHv1 only, read access); Diffie-Hellman key pair for SSHv2 key exchange (read/write access); session key for SSH (read/write access); X9.31 PRNG keys (read access)
TLS	Provide authenticated and encrypted sessions while using the Check Point management interface	TLS handshake parameters, TLS inputs, and data	TLS outputs and data	RSA key pair for TLS key transport (read access); session keys for TLS (read/write access); X9.31 PRNG keys (read access)
Boot manager commands	Control the boot-up process and obtain system information	Commands and configuration data	Status of commands and configuration data	Password (read/write access)
SNMPv3 Get commands	View MIB values	Commands	Status of commands, configuration data	Password (read access)

Table 3 Crypto Officer Services, Descriptions, Inputs, and Outputs

Service	Description	Input	Output	Critical Security Parameter (CSP) access
Interface commands	Configure, manage, and view physical and logical interfaces through the CLI: View all interfaces; delete any logical interface; view tunnels; view status and statistics; configure ARP behavior, physical and logical ATM interfaces, physical and logical Ethernet interfaces, physical and logical FDDI interfaces, physical and logical ISDN interfaces, physical or logical loopback interfaces, and physical and logical serial interfaces	Commands and configuration data	Status of commands and configuration data	

Table 3 Crypto Officer Services, Descriptions, Inputs, and Outputs

Service	Description	Input	Output	Critical Security Parameter (CSP) access
Routing commands	Configure, manage, and view the routing protocols through the CLI: Configure, manage, and view BGB, OSPF, RIP, IGRP, IGMP, PIM, route aggregation, BOOTP, DVMRP, static routes, VRRP, ICMP router discovery, IP broadcast helper, Network Time Protocol, and dial on demand routing; configure a variety of miscellaneous options that affect routing; configure trace routing settings; view summary information about routes on the system; view general information that the IPSO routing daemon records; view information about multicast forwarding cache	Commands and configuration data	Status of commands and configuration data	None

Table 3 Crypto Officer Services, Descriptions, Inputs, and Outputs

Service	Description	Input	Output	Critical Security Parameter (CSP) access
Network Security and Access commands	Configure, manage, and view the security and access features through the CLI: Configure and view network access; add software licenses to the platform; configure Authentication, Authorization, and Accounting (AAA); enable and disable and configure SSH services; add and delete new system users; create and delete groups, and add and remove members; enable and disable a VPN accelerator card; display VPN accelerator status or statistics	Commands and configuration data	Status of commands and configuration data	Admin, monitor, user passwords; shared secret for RADIUS; shared secret for TACPLUS; SSH host keys; SSHv1 server key; SSH User identity keys; SSH authorized keys; Read/write access for all CSPs

Table 3 Crypto Officer Services, Descriptions, Inputs, and Outputs

Service	Description	Input	Output	Critical Security Parameter (CSP) access
Traffic management commands	Configure, manage, and view traffic management functionality through the CLI: Configure an access list to control the traffic from one or more interfaces; create or delete existing aggregation classes and modify the mean rate or burst size; configure depth of queues, assign logical names to some of the queues, and set up a queue specifier; add, delete, or show ATM QoS descriptors; add, delete, or show association of ATM QoS descriptors with ATM VCs; show available or reserved bandwith on an ATM interface; enable and disable DSCP to VLAN mapping	Commands and configuration data	Status of commands and configuration data	None

Table 3 Crypto Officer Services, Descriptions, Inputs, and Outputs

Service	Description	Input	Output	Critical Security Parameter (CSP) access
System configuration commands	Configure, manage, and view system configuration settings through the CLI: View the platform configuration; configure the system to perform manual or regularly scheduled backups; schedule regular jobs; configure system failure; configure domain name and domain name servers; configure static host names for particular IP addresses; configure host name of platform; manage IPSO images; manage configuration sets; manage relay configuration; configure network system logging; configure the date and time; view date and time settings; view the disks that IPSO detects on local system; specify other systems as network time protocol servers or peers; display information about packages installed on the local system	Commands and configuration data	Status of commands and configuration data	None

Table 3 Crypto Officer Services, Descriptions, Inputs, and Outputs

Service	Description	Input	Output	Critical Security Parameter (CSP) access
SNMP commands	Configure, manage, and view SNMP settings through the CLI: Configure SNMP parameters; enable and disable SNMP; add users who are authorized to use SNMPv3; show SNMP implementation commands; show SNMPv3 user commands	Commands and configuration data	Status of commands and configuration data	Password (read/write access)
IPv6 commands	Configure, manage, and view IPv6 settings through the CLI: Show a summary of IPv6 configuration; associate and disassociate an IPv6 address with a logical interface, anycast address, or IPv6 address family; map and IPv6 address to a physical machine address recognized in the local network; create tunnels by using specific encapsulation schemes; configure and delete an IPv6 interface to IPv4 interface; create, enable, or disable an IPv6 interface attached to an IPv4 network that does not have IPv6 native support; configure IPv6 routing; add and delete logical IPv6 hosts; enable and disable network access and view current status of network access	Commands and configuration data	Status of commands and configuration data	None

Table 3 Crypto Officer Services, Descriptions, Inputs, and Outputs

Service	Description	Input	Output	Critical Security Parameter (CSP) access
Monitoring commands	Configure, manage, and view monitoring settings through the CLI: Configure CPU use reports, memory use reports, interface linkstate reports, rate shaping bandwidth reports, interface throughput reports by turning data collection on or off and setting the data collection time interval; display interface settings, system logs, system statistics, interface monitor, resource statistics, forwarding table, system status information	Commands and configuration data	Status of commands, configuration data, and status information	None
Check Point CLI commands	Initial configuration of the Check Point software: Install licenses, configure the SNMP daemon, modify the list of UNIX groups authorized to run VPN-1/FW-1 services, register a cryptographic token, enter random data to help seed the PRNG, configure the one-time SIC password, and specify whether the VPN-1/ FW-1 services should automatically start at boot time	Command (cpconfig), menu options, and configuration information	Status of commands and menu options and status information (configuration information)	One-time SIC password (read/write

Table 3 Crypto Officer Services, Descriptions, Inputs, and Outputs

Service	Description	Input	Output	Critical Security Parameter (CSP) access
Check Point SmartDashBoard services	Create and configure users and user groups:define users and user groups; create permission for individual users or a whole group of users; set permissions such as access hours, user priority, authentication mechanisms, protocols allowed, filters applied, and types of encryption	Commands and configuration data (policy files)	Status of commands and configuration data (policy files)	None
	Define and implement security policies: Configure and installation security policies that are applied to the network and users. These policies contain a set of rules that govern the communications flowing into and out of the module, and provide the Crypto Officer with a means to control the types of traffic permitted to flow through the module.	Commands and configuration data (policy files)	Status of commands and configuration data (policy files)	None
	Management of keys: Configure the digital certificates and/or preshared keys for use by IPSec and IKE for authentication	Commands and configuration data (policy files)	Status of commands and configuration data (policy files)	RSA key pair for IKE (read/write access); preshared keys for IKE (read/write access)
	Initialization of Secure Internal Communication (SIC): Establish trust between management server and the module to allow configuration of the module's services	Commands and configuration data (SIC policy)	Status of commands	RSA key pair for TLS (read/write access)

Table 3 Crypto Officer Services, Descriptions, Inputs, and Outputs

Service	Description	Input	Output	Critical Security Parameter (CSP) access
	RSA key pair for IKE (read/write access); preshared keys for IKE (read/write access)	Commands and configuration data (SIC policy)	Status of commands	RSA key pair for TLS (read/write access)
	Monitoring:provides detailed information for both monitoring of connection activities and the system status	Commands	Status of commands and status information (logs)	None

User Role

The User role accesses the module IPSec and IKE services. Service descriptions, inputs, and outputs are listed in Table 4.

Table 4 User Services, Descriptions, Inputs, and Outputs

Service	Description	Input	Output	CSP
IKE	Access the module IKE functionality to authenticate to the module and negotiate IKE and IPSec session keys	IKE inputs and data	IKE outputs, status, and data	RSA key pair for IKE (read-only access); Diffie-Hellman key pair for IKE (read/write access); preshared keys for IKE (read-only access)
IPSec	Access the module IPSec services to secure network traffic	IPSec inputs, commands, and data	IPSec outputs, status, and data	Session keys for IPSec (read/write access)

Authentication Mechanisms

The modules implement password-based authentication, RSA-based authentication, DSA-based authentication, and HMAC-based authentication mechanisms.

Crypto Officer Authentication

The Crypto Officer must successfully authenticate before a management interface can be accessed. The following are authentication methods:

- **CLI (local)–**the Crypto Officer must authenticate by using user ID and password. The password must be at least six characters long. Numeric, alphabetic (upper and lowercase), and keyboard and extended characters can be used.
- **CLI (remote)–**the Crypto Officer must first successfully authenticate during the SSH session establishment. Since no digital certificates are used, the Crypto Officer must login locally at initialization through the CLI and enter the authorized RSA or DSA public key. The Crypto Officer then uses this public key to authenticate during the SSH session establishment. Once a session is established, the Crypto Officer must successfully authenticate by using the user ID and password before the management interface can finally be accessed.
- **SNMP–**the Crypto Officer must authenticate by using the user ID and password. It is the same password used to access the CLI. The only restriction is that the password must be at least eight characters long.
- **SmartDashBoard–**during the TLS session establishment the Crypto Officer must authenticate by using a digital certificate that contains the Crypto Officer RSA public key. The authenticity of the digital certificate is guaranteed by the inclusion of the digital signature of the issuing Certification Authority (CA).

User Authentication

User authentication to the module is performed during IKE using digital certificates or preshared keys. The digital certificates contain the User RSA public keys and are signed by the private key of the CA. The preshared keys must be at least six characters long and use at least four different characters.

Estimated Strength of the Authentication Mechanisms

The estimated strength of each authentication mechanism implemented by the module is described in Table 5.

Table 5 Estimated Strength of Authentication Mechanisms

Authentication type	Strength
DSA-based authentication (SSHv2)	DSA signing and verification is used to authenticate to the module during SSHv2. This mechanism is as strong as the DSA algorithm using a 1024-bit key pair.
RSA-based authentication (SSHv1 and TLS handshake)	RSA encryption and decryption is used to authenticate to the module during SSHv1 and the TLS handshake. This mechanism is as strong as the RSA algorithm using a 1024-bit key pair.
RSA-based authentication (IKE)	RSA signing and verification is used to authenticate to the module during IKE. This mechanism is as strong as the RSA algorithm using a 1024-bit key pair.
Preshared key-based authentication (IKE)	SHA-1 HMAC generation and verification is used to authenticate to the module during IKE with preshared keys. This mechanism is as strong as the HMAC with SHA-1 algorithm. Additionally, preshared keys must be at least six characters long and use at least four different characters. Even if only uppercase letters were used without repetition for a six character preshared key, the probability of randomly guessing the correct sequence is one in 165,765,600.
Password-based authentication	Passwords are required to be at least six characters long. Numeric, alphabetic (upper and lowercase), and keyboard and extended characters can be used, which gives a total of 95 characters to choose from. Considering only the case-insensitive alphabet using a password with repetition, the number of potential passwords is 26^6.

Physical Security

The Nokia IP350 and IP380 appliances are multichip standalone cryptographic modules, which were tested and found to comply with the limits for a Class A digital device, pursuant to Part 15 of the FCC rules.

The modules are entirely contained within hard metal enclosures. The enclosure is resistant to probing and is opaque within the visible spectrum. The front and side vent holes are baffled from the inside using lance wall inserts.

The metal case can be disassembled by loosening the two front thumbscrews and sliding the chassis assembly forward. Unscrewing the screws on top of the case does not remove the top cover, since the top cover is locked into position and must be moved forward to unlock it. Hence, the internal of the module can only be viewed by sliding the chassis assembly forward. One tamper-evident seal is therefore required to provide protection and to notify of any tampering with the modules. The tamper-evident seal is employed by the Crypto Officer as described in "Crypto Officer Guidance" on page 33.

Operational Environment

The operational environment requirements do not apply to these modules. The Nokia IP350 and IP380 appliances do not provide a general-purpose operating system nor does it provide a mechanism to load new software.

Cryptographic Key Management

Cryptographic algorithms are implemented in software by IPSO and Check Point VPN-1 and in hardware by the encryption accelerators.

The IPSO operating system provides the capability to use SSHv1 or SSHv2 to secure the remote CLI management sessions. The implemented FIPS-approved algorithms include RSA (SSHv1) and DSA (SSHv2) for authentication, Triple-DES for data encryption, SHA-1 for data hashing, and HMAC SHA-1 for data packet integrity. Key establishment is performed by using the RSA key transport for SSHv1 and the Diffie-Hellman key agreement for SSHv2.

Check Point provides the capability to use TLSv1 to secure the Web-based management sessions. The implemented FIPS-approved algorithms include RSA for authentication; DES, Triple-DES, and AES for data encryption; SHA-1 for data hashing; and HMAC SHA-1 for data packet integrity. Key establishment is performed by using the RSA key transport. The VPN-1 module supports IPSec/ESP for data encryption, IPSec/ESP for data integrity, and IPSec/AH for data integrity. The VPN-1 module implements all IKE modes: main, aggressive, and quick, using ISAKMP according to the standard.

The hardware encryption accelerators provide the VPN-1 module with fast DES, Triple-DES, HMAC SHA-1, and Diffie-Hellman modular exponentiation processing. The Broadcom BCM5802 provides accelerated IPSec processing for both the Nokia IP350 and IP380. In addition to the BCM5802, the IP380 supports the optional BCM5805 for even better VPN performance. The two accelerators provide the same functionalities, differing only in performance levels.

To summarize, the modules implement the following FIPS-approved algorithms (for the certificate numbers of the validated FIPS-approved algorithms, see Appendix B, "Certificate Numbers"):

Data encryption:

- Advanced Encryption Standard (AES) in CBC mode (128 or 256 bit keys) – according to NIST FIPS PUB 197.

- Data Encryption Standard (DES) in CBC mode (56 bit keys) (for legacy use only)–according to NIST PUB FIPS 46-2.
- Triple DES (3DES) in CBC modes (168 bit keys)–according NIST PUB FIPS 46-2.

Data packet integrity:

- HMAC-SHA-1 (20 byte)–according to NIST PUB FIPS 198, RFC 2104 (HMAC: Keyed-Hashing for Message Authentication), and RFC 2404 (using HMAC-SHA-1-96 within ESP and AH).

Data hashing:

- Secure Hash Algorithm (SHA-1)–according to NIST PUB FIPS 180-1

Digital signature:

- Digital Signature Algorithm (DSA)–according to FIPS 186-2 Change Notice 1

PRNG:

- ANSI X9.31-based PRNG with Yarrow controls on entropy gathering

The module implements the following algorithms permitted for use in a FIPS-approved mode of operation.

Digital signatures and key transport:

- RSA–according to PKCS #1

Session security:

- SSHv1 (configured to use FIPS-approved algorithms)
- SSHv2 (configured to use FIPS-approved algorithms)
- TLS v1.0 (configured to use FIPS-approved algorithms) - according to RFC 2246
- IPSec (configured to use FIPS-approved algorithms)

Key exchange:

- Diffie-Hellman (used by IKE and SSHv2)

The module also implements the following PRNGs, which are not used for cryptographic purposes:

- ARC4-based PRNG
- Simple Linear Congruential PRNG

The module supports the critical security parameters listed in Table 6.

Table 6 Listing CSPs for the Module

CSPs	CSPs type	Generation	Storage	Use
Host RSA key pair	1024-bit RSA private- and public-key pair	Internal—using X931 PRNG	Stored in plaintext on disk	SSH server authentication and key transport to client (SSHv1)
Host DSA key pair	160-bit DSA private key and 1024-bit DSA public key	Internal—using X931 PRNG	Stored in plaintext on disk	SSH server authentication to client (SSHv2)
Server RSA key pair	512-, 640-, 768- (default), 864-, 1024-bit private- and public-key pair	Internal—using X931 PRNG	Stored in plaintext on disk	SSH server authentication and key transport to client (SSHv1)
User RSA key pair	1024-bit RSA private- and public-key pair	Internal—using X931 PRNG	Stored in plaintext on disk	Client authentication to other SSH servers (SSHv1)
User DSA key pair	160-bit DSA private key and 1024-bit DSA public key	Internal—using X9.31 PRNG	Stored in plaintext on disk	Client authentication to other SSH servers (SSHv2)
Authorized RSA key	1024-bit RSA public key	External	Stored in plaintext on disk	Client authentication to other SSH servers (SSHv1)
Authorized DSA key	1024-bit DSA public key	External	Stored in plaintext on disk	Client authentication to other SSH servers (SSHv2)
TLS RSA key pair	1024-bit RSA private- and public-key pair	External	Stored in plaintext on disk	TLS server authentication and key transport during TLS handshake
TLS client RSA public key	1024-bit RSA public key	External	Stored in plaintext on disk	Client authentication during TLS handshake
IKE RSA key pair	1024-bit RSA private- and public-key pair	External	Stored in plaintext on disk	Server authentication during IKE
IKE client RSA public key	1024-bit RSA public key	External	Stored in plaintext on disk	Server authentication during IKE
Preshared keys	6-character preshared key	External	Stored in plaintext on disk	Client ande server authentication during IKE

Table 6 Listing CSPs for the Module

CSPs	CSPs type	Generation	Storage	Use
IKE Diffie-Hellman key pair	768-, 1024-, 1536-bit Diffie-Hellman private- and public-key pair	External	Stored in plaintext on disk	Key agreement during IKE
IKE client Diffie-Hellman public key	768-, 1024-, 1536-bit Diffie-Hellman public key	External	Stored in plaintext on disk	Key agreement during IKE
SSHv2 Diffie-Hellman key pair	Up to 2048-bit Diffie-Hellman private/public key pair	Internal–using X9.31 PRNG	Stored in plaintext on disk	Key agreement during SSHv2
SSHv2 client Diffie-Hellman public key	Up to 2048-bit Diffie-Hellman public key	External	Stored in plaintext on disk	Key agreement during SSHv2
SSH session keys	168-bit TDES keys; HMAC SHA-1 keys	Established during the SSH key exchange by using RSA key transport (SSHv1) or Difie-Hellman key agreement (SSHv2)	Stored in plaintext on disk	Secure SSH traffic
TLS session keys	56-bit DES or 168-bit TDES keys; HMAC SHA-1 key	Established during the TLS handshake by using RSA key transport	Cached to disk	Secure TLS traffic
IPsec session keys	56-bit DES, 128-bit TDES, or 128-, 256-bit AES keys; HMAC SHA-1 key	Established during the Diffie-Hellman key agreement	Stored in plaintext on disk	Secure IPSec traffic
IPSO X9.31 PRNG keys	128-bit TDES keys	Internal—by gathering entropy	Stored in plaintext on disk	IPSO psuedo-random number generator forRSA, DSA, Diffie-Helman keys
Check Point X9.31 PRNG keys	128-bit TDES keys	Internal–by gathering entropy	Stored in plaintext in memory, but entropy used to generate keys is cached to disk	Check Point pseudo-random number generator for Diffie-Hellman keys
Passwords	Six-character password (SNMPv3 requires at least eight characters)	External	Stored in plaintext on disk	Authentication for accessing the management interfaces (CLI and SNMPv3); boot manager authentication; RADIUS authentication; TACPLUS authentication

Key Generation

The only keys that can be generated by the modules are RSA and DSA public and private keys for SSHv1 and SSHv2, respectively, and Diffie-Hellman secret and public values for SSHv2 and IPSec. The FIPS-approved X9.31 PRNG is used to generate these keys.

Key Establishment

The modules implement IKE, SSH, and the TLS handshake for automatic key establishment. Two types of key establishment techniques are employed by the modules: the Diffie-Hellman key agreement and the RSA key transport. The Diffie-Hellman key agreement establishes shared secrets during SSHv2 and IKE. The RSA key transport generates shared secrets during SSHv1 and TLS.

Key Entry and Output

All private and secret keys entered into the module are electronically entered. No private and secret keys are output from the module.

Key Storage

All RSA (except the server key) and DSA keys, preshared keys, and passwords are stored in plaintext on disk. The TLS session keys and the gathered entropy for the Check Point PRNG keys are cached to disk. All other keys are ephemeral keys and are stored in plaintext in memory.

Key Zeroization

Ephemeral keys can be zeroized by rebooting. All other keys can be zeroized by overwriting or deleting them.

Self-Tests

The modules perform a set of self-tests to ensure proper operation in compliance with FIPS 1402. These self-tests are run during power-up (power-up self-tests) or when certain conditions are met (conditional self-tests).

Power-up self-tests:

- Software integrity tests: the modules use a CRC-32 to check the integrity of its various components
- Cryptographic algorithm tests:
  - AES-CBC KAT
  - DES-CBC KAT
  - Triple-DES-CBC KAT

  - PRNG KAT
  - RSA pair-wise consistency test (encryption and decryption)
  - RSA pair-wise consistency test (signing and verification)
  - RSA KAT (signing and verification)
  - DSA pair-wise consistency test
  - SHA-1 KAT
  - SHA-1 HMAC KAT
- Policy file integrity test (bypass mode test): the module performs a SHA-1 check value verification to ensure that the policy files are not modified.

Conditional self-tests:

- RSA pair-wise consistency test. This test is performed when RSA keys are generated for SSHv1.
- DSA pair-wise consistency test: this test is performed when DSA keys are generated for SSHv2.
- Continuous random number generator tests: these tests are constantly run to detect failure of the random number generators of the module.
- Policy file integrity test (bypass mode test): the module performs a SHA-1 check value verification to ensure that the policy files are not modified.

If the software integrity tests fail, the module enters the bootloader error state and reboots. If the IPSO kernel modules cryptographic algorithm tests fail, the module enters the kernel panic error state and reboots. If the Check Point kernel module cryptographic algorithm tests fail, the module enters the kernel panic error state and must be rebooted by the Crypto Officer to clear the error.

If the IPSO conditional self-tests fail, the module enters the error state and reboots. If the Check Point continuous RNG test fails, the module enters the error state and reboots. All other self-test errors cause the module to enter the error state, where all cryptographic services and data output for the problem service is halted until the error state is cleared. Restarting the module or the failed service can clear the error state.

All errors are logged and produce error indicators.

Design Assurance

Nokia and Check Point manage and record source code and associated documentation files by using the Concurrent Versions System (CVS).

The Nokia hardware data, which includes description, part data, part type, bill of materials, manufacturers, changes, history, and hardware documents are managed and recorded using Agile Workplace.

Additionally, Microsoft Visual Source Safe (VSS) version 6.0 was used to provide configuration management for the module's FIPS documentation. This software provides access control, versioning, and logging.

Mitigation of Other Attacks

The modules do not employ security mechanisms to mitigate specific attacks.

2 Secure Operation

The Nokia IP350 and IP380 meet Level 2 requirements for FIPS 140-2. The following sections describe how to place and keep the module in FIPS-approved mode of operation. The Crypto Officer must ensure that the module is kept in a FIPS-approved mode of operation. The procedures are described in "Crypto Officer Guidance."

The User can use the module after the Crypto Officer changes the mode of operation to FIPS mode and enables the Check Point modules. The secure operation for the User is described in "User Guidance" on page 43.

Crypto Officer Guidance

The secure operation procedures include the initial setup, configuring the Check Point modules in a FIPS compliant manner, and keeping the module in a FIPS-approved mode of operation. These procedures are described in the following sections.

Initial Setup

The Crypto Officer receives the module in a carton. Within the carton the module is placed inside an ESD bag; two foam end caps are placed on both sides of the chassis, protecting the module during shipping. The Crypto Officer should examine the carton and the ESD bag for evidence of tampering. Tamper-evidence includes tears, scratches, and other irregularities in the packaging.

Since the module does not enforce an access control mechanism before it is initialized, the Crypto Officer must maintain control of the module at all times until the initial setup is complete.

Before turning on the module, the Crypto Officer must ensure that the module meets Level 2 physical security requirements. To satisfy these requirements, the Crypto Officer must install the tamper-evident seal provided in the FIPS kit—N431174001 (12 pieces). After the seal is in place, the Crypto Officer must initialize the module and set the module to FIPS mode.

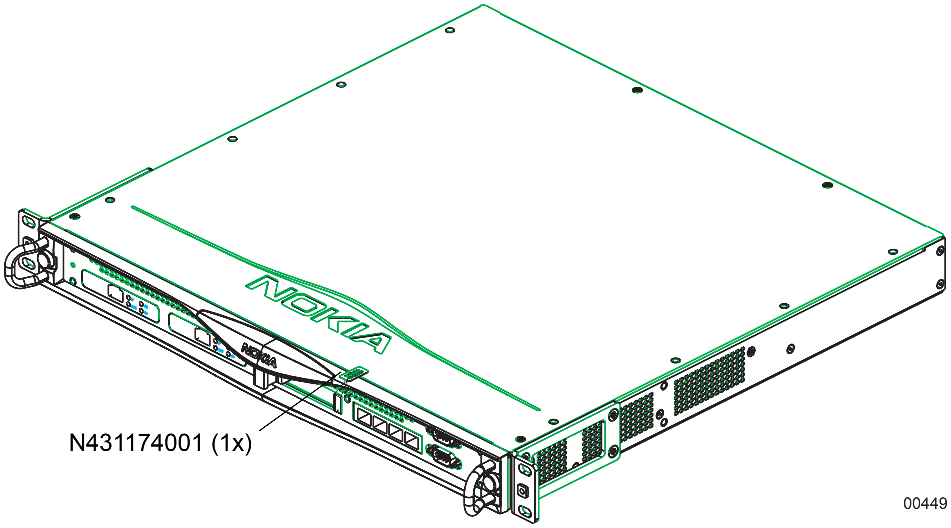
Applying the Tamper-Evident Seal

One tamper-evident seal is required to protect and detect tampering of the module.

To apply the serialized seal

1. Apply the seal on the top front, overlapping the main chassis and the front panel.

> **Note**
> Use only one of the pieces of sealing tape.



2. Record the serial number of the applied seal in a security log.
3. Allow 24 hours for the adhesive in the tamper-evident seal to completely cure.

Initializing the System

Before performing the initial configuration, the Crypto Officer must set the boot manager password to prevent unauthorized access to the module hard disk.

To initialize the appliance

Perform the following steps. For more information, see the *IPSO 3.7.99 Installation Guide*.

1. Establish a physical console connection to the appliance.

   The console can be any standard VT100-compatible terminal or terminal emulator with the following properties:

   - RS-232 data terminal equipment (DTE)
   - 9600 bps
   - 8 data bits
   - No parity
   - 1 stop bit

   You can also use a data communications equipment (DCE) device.

To establish the physical console connection, follow these steps:

a. Connect the appropriate cable to the local console port on the front panel of the appliance.

   If the console is DTE, use the supplied null-modem cable (console cable). If the console is DCE, use a straight-through cable.

b. Connect the other end of the cable to the console system.

2. Turn the appliance on.
3. When the system enters autoboot mode and displays the following message, press any key to display the boot manager prompt:

   ```
   Type any character to enter command mode
   ```

4. At the boot manager prompt, enter

   ```
   passwd
   ```

5. At the prompt, enter a new password.
6. At the prompt, re-enter the new password for verification.
7. Start IPSO by entering

   ```
   boot
   ```

8. After it boots, the system prompts you to provide a host name and IP address.

   Enter this information as appropriate.

9. When prompted, reboot the system by entering `reboot` to make the changes take effect.

Installing or Upgrading the Check Point NG with AI R54 Module

The modules come preinstalled with the Check Point FP3 HF2 module. The Crypto Officer must either delete this version and install the NG with AI R54 version, or upgrade the FP3 HF2 version to the NG with AI R54 version.

To delete the existing FP3 HF2 packages

1. From Voyager, the Web-based management interface, click the Manage Installed Packages link in the System Configuration section.
2. Turn off Check Point VPN-1/Fire Wall-1 NG Feature Pack 3.
3. Turn off Check Point SVN Foundation NG Feature Pack 3.
4. Click the Delete Packages link.
5. Click DELETE next to the packages.
6. Click APPLY.
7. Click SAVE to make your changes permanent.
8. From the system console exit and log in again.

Use the following instructions to install the NG with AI R54 packages

To upgrade when FP3 HF2 is already installed but firewall is not configured

1. From Voyager, the Web-based management interface, click the *Manage Installed Packages* link
2. Ensure that only Check Point VPN-1/Fire Wall-1 NG Feature Pack 3 and Check Point SVN Foundation NG Feature Pack 3 are present and turned on.
3. From the system console, issue the *cpconfig* command and follow the instructions.

   Be sure to choose the following options during cpconfig: Distributed installation (option 2) and Enforcement module (option 1).
4. At the prompt, reboot the system.

   After the reboot, the system starts with the default policy.
5. After logging on, use the following instructions to upgrade the packages to NG with AI R54.

To install or upgrade Check Point NG with AI R54 packages from the system console

1. FTP (with user ID and password) the Check Point packages to the system from a remote location and place them under any directory, preferably /opt/packages.

   For additional security, choose SFTP or SCP for transferring the file.
2. From the system console, issue the command newpkg and select option *4*.
3. At the prompt, enter the pathname (for instance, /opt/packages).
4. Choose option 1 to install the NG with AI R54 package or option 2 to upgrade the package to NG with AI R54 from FP3 HF2.
5. After the installation or upgrade is complete, reboot.

Setting the Module to FIPS Mode

Before proceeding, the Crypto Officer must set the mode of operation to FIPS mode.

To set the mode of operation to FIPS mode

1. Using a console connection, start the IPSO CLI by entering **`clish`**.

1. At the CLI prompt, enter the **`set fips on`** restart command.
2. If desired, enter the **`show fips`** command to view the current list of features that are disabled and enabled.

   For the list of disabled access and feature mechanisms, see Appendix A, “Disabled Mechanisms.”

Initializing the Remote Management of the Module

Before the Crypto Officer can manage the module remotely, SSH must be enabled, the Crypto Officer’s public key must be entered, and only FIPS-approved algorithms can be selected.

To initialize the remote management of the module

1. Using the CLI through the console port, enter the **`set ssh server enable 1`** command.
2. To ensure that the Crypto Officer can log in (with a password) using SSH, enter the following command:

   ```
   set ssh server permit-root-login yes
   ```

3. Configure the type of authentication that the server will use to authenticate the Crypto Officer by entering the following commands:

   ```
   set ssh server
         dsa-authentication 1
         password-authentication 1
         rhosts-authentication 0
         rhosts-authentication 0
         rsa-authentication 1
   ```

4. Allow only FIPS-approved algorithms for encryption and configure the SSH protocol by entering the following commands:

   ```
   set ssh server
         ciphers 3des-cbc
         keepalives <0 | 1>
         listen-addr ip_address
         listen-addr2 ip_address
         port  <1 | 2 | 1,2>
         server-key-bits 1024
   ```

5. Generate host keys for either SSHv1, SSHv2, or both by entering the following commands:

   ```
   set ssh server
         v1 size 1024
         v2 dsa size 1024
   ```

6. Enter the Crypto Officer's authorized public key for SSHv1, SSHv2, or both with the following commands:

   ```
   add ssh authkeys
         v1 user name bits integer exponent integer modulus name
           comment name
         v2 dsa user name <openssh-format name | ssh2-format file name>
           comment name
   ```

For optional configuration settings, see the *CLI Reference Guide for IPSO 3.7*.

The module can now be managed remotely with SSH-secured management sessions.

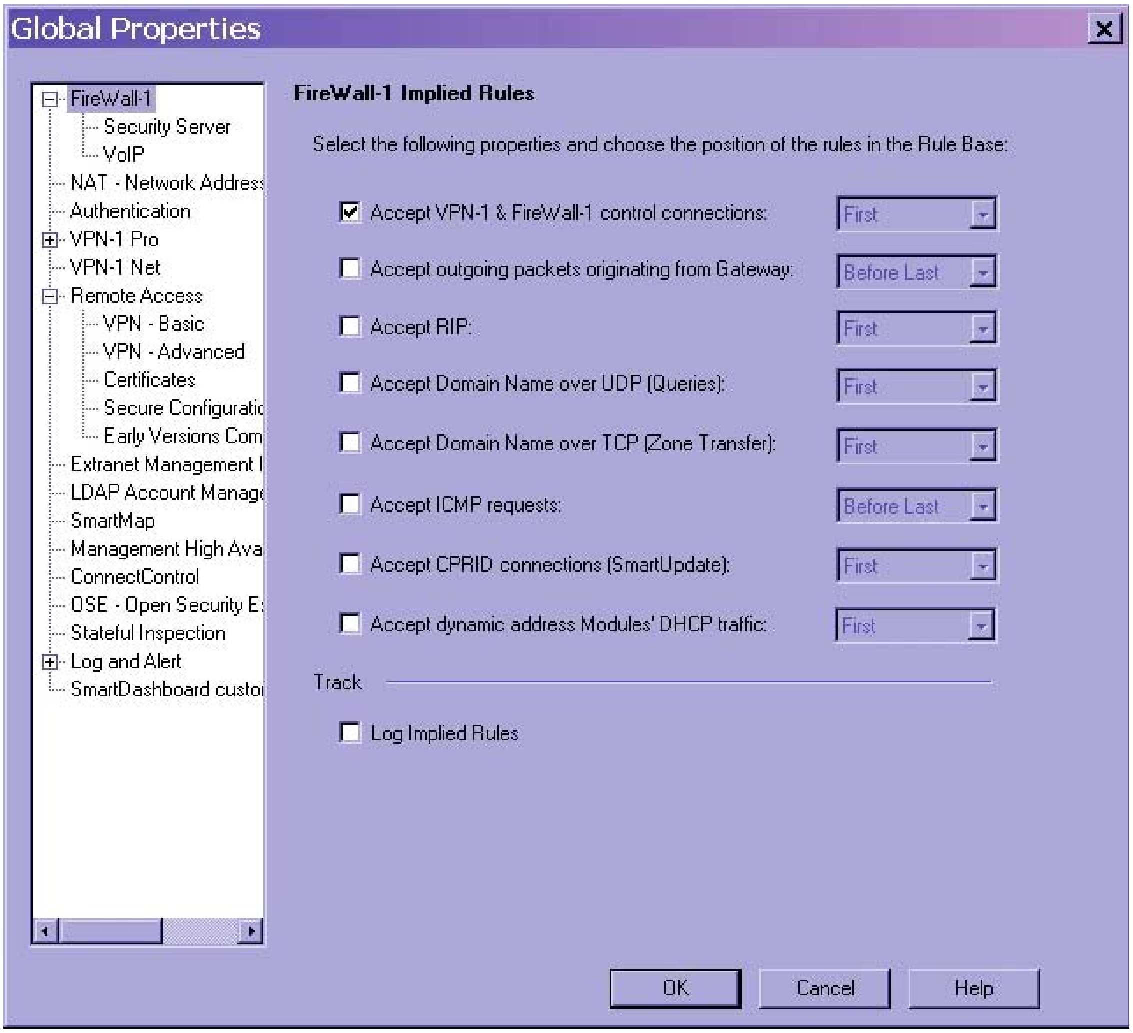
When changing the configuration, the preceding settings denoted by bold letters and numbers must not be changed.

Initializing Check Point Modules

Before the User can use the FW-1 and VPN-1 functionalities, the Check Point module must be enabled and initialized using the CLI. The initialization process requires that the Crypto Officer establishes the SIC configuration. Once this is completed, the module is adequately initialized and can be managed from the management server.

If not completed already, turn FIPS mode on. After this process is complete and remote management of the module is available (that is, SIC is initialized), the FireWall-1 implied rules must be configured through SmartDashboard as depicted in Figure 6. Check the Accept VPN-1 & FireWall-1 control connections check box, select: First in the pull-down list, and click OK.

Figure 3 Implied Rules for FireWall-1



FireWall-1 Implied Rules

Select the following properties and choose the position of the rules in the Rule Base:

☑ Accept VPN-1 & FireWall-1 control connections: First

☐ Accept outgoing packets originating from Gateway: Before Last

☐ Accept RIP: First

☐ Accept Domain Name over UDP (Queries): First

☐ Accept Domain Name over TCP (Zone Transfer): First

☐ Accept ICMP requests: Before Last

☐ Accept CPRID connections (SmartUpdate): First

☐ Accept dynamic address Modules' DHCP traffic: First

Track

☐ Log Implied Rules

Management

After the initial setup, the Crypto Officer can locally or remotely manage, configure, and monitor the IPSO module with the CLI, or monitor with SNMPv3. Once initialization of the Check Point module is complete, the Crypto Officer can manage the Check Point module with the remote management server. Through this server, the Crypto Officer can configure policies for the module. These policies determine how the firewall and VPN services of the module function.

During the management of the module, the Crypto Officer must satisfy the following:

- The SSH configuration settings specified in Section 3.1.1.6 must be satisfied.
- Authorized public keys must be entered into the module with the SSH-secured management session.
- The AUX port must not be enabled.
- The module logs must be monitored. If a strange activity is found, the Crypto Officer should take the module off line and investigate.
- The tamper-evident seal must be regularly examined for signs of tampering.

The VPN functionality must be configured to use only FIPS-approved algorithms. Authentication during IKE must employ preshared keys or digital certificates. IPSec and IKE can use only the following FIPS-approved algorithms:

Data encryption:

- DES (for legacy use only)
- Triple DES
- AES

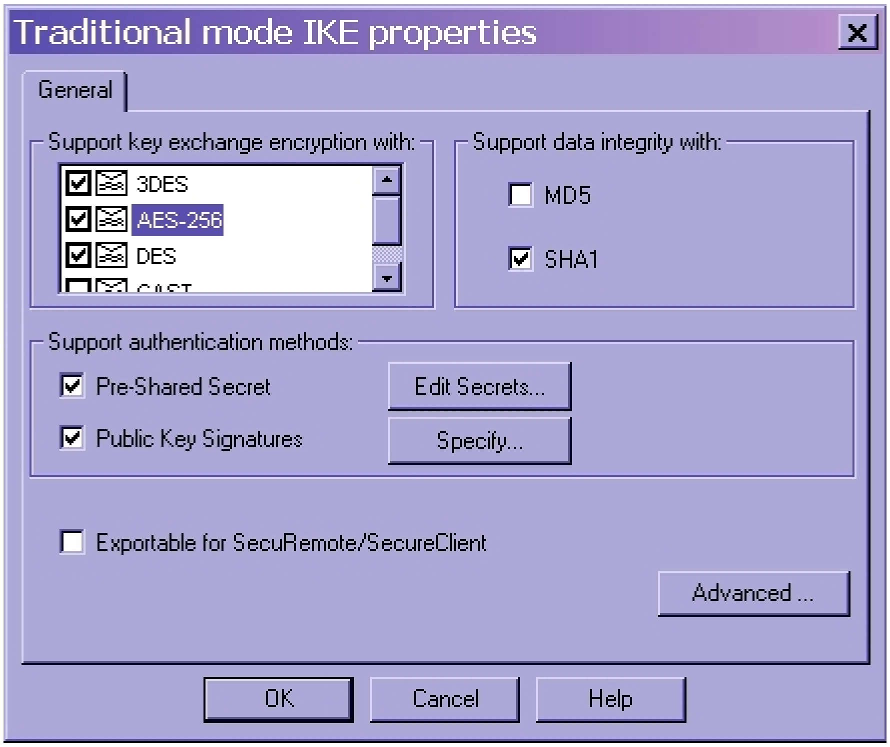
Data packet integrity:

- HMAC with SHA1

Authentication:

- Certificates
- Preshared keys

Figure 4 Only FIPS-Approved Algorithms Can Be Used with IKE



Traditional mode IKE properties

General

Support key exchange encryption with:

- ☑ 3DES
- ☑ AES-256
- ☑ DES
- □ CAST

Support data integrity with:

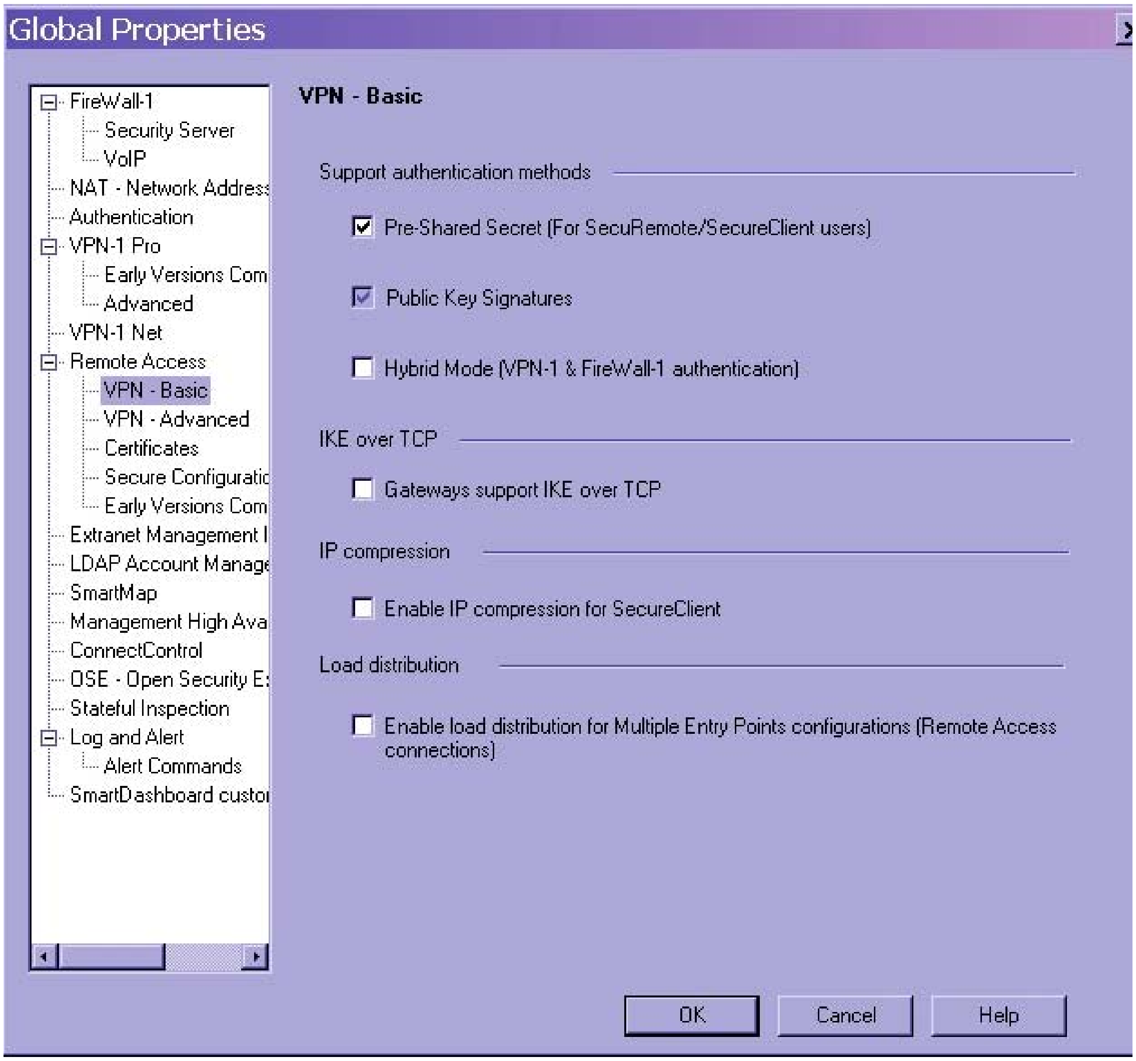
- □ MD5
- ☑ SHA1

Support authentication methods:

- ☑ Pre-Shared Secret
- ☑ Public Key Signatures

□ Exportable for SecuRemote/SecureClient

Figure 5 Only Preshared Keys or Digital Certificates Can Be Used to Authenticate Clients



VPN - Basic

Support authentication methods

☑ Pre-Shared Secret (For SecuRemote/SecureClient users)

☑ Public Key Signatures

□ Hybrid Mode (VPN-1 & FireWall-1 authentication)

IKE over TCP

□ Gateways support IKE over TCP

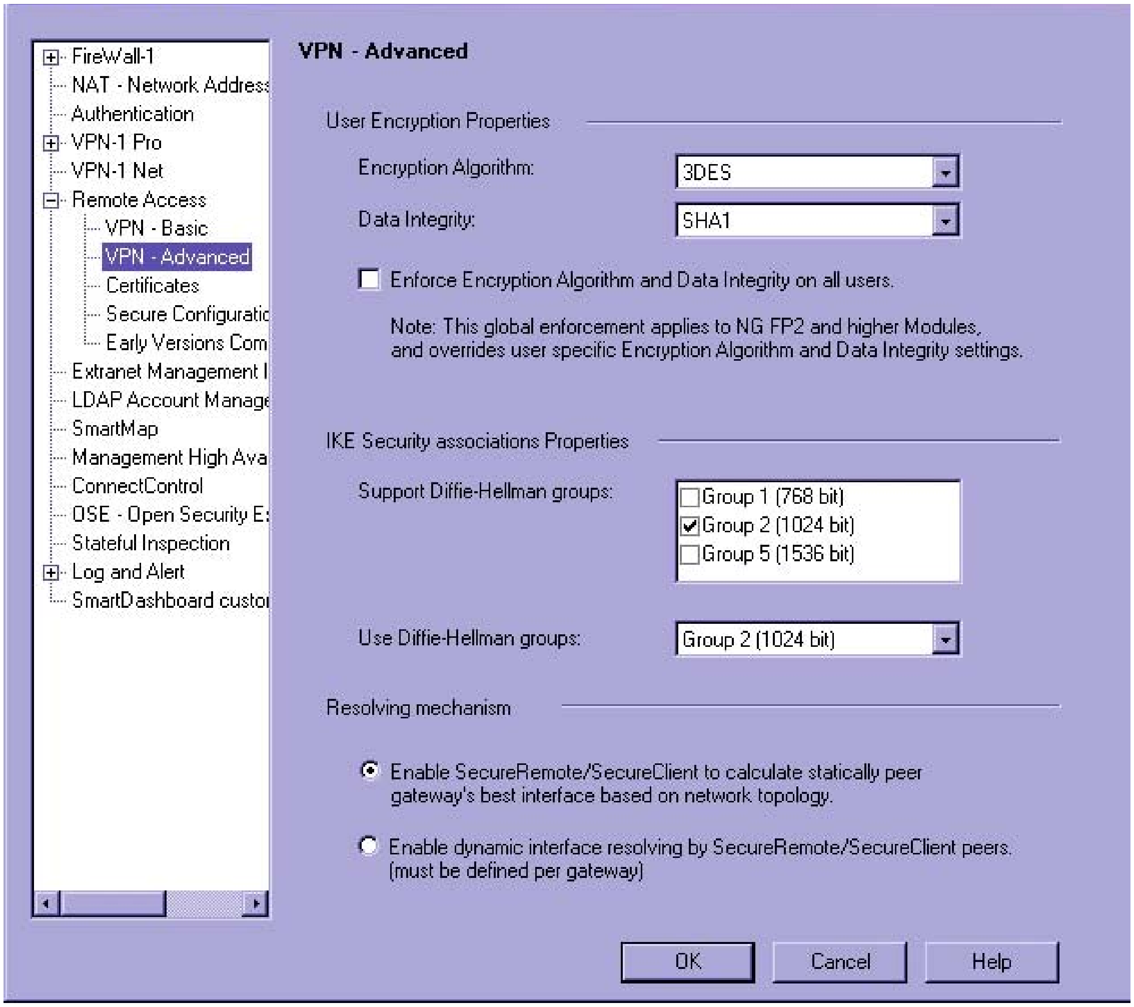
IP compression

□ Enable IP compression for SecureClient

Load distribution

□ Enable load distribution for Multiple Entry Points configurations (Remote Access connections)

Figure 6 Only FIPS-Approved Algorithms Can Be Used with IPSec



VPN - Advanced

User Encryption Properties

Encryption Algorithm: 3DES

Data Integrity: SHA1

□ Enforce Encryption Algorithm and Data Integrity on all users.

Note: This global enforcement applies to NG FP2 and higher Modules, and overrides user specific Encryption Algorithm and Data Integrity settings.

IKE Security associations Properties

Support Diffie-Hellman groups:
□ Group 1 (768 bit)
☑ Group 2 (1024 bit)
□ Group 5 (1536 bit)

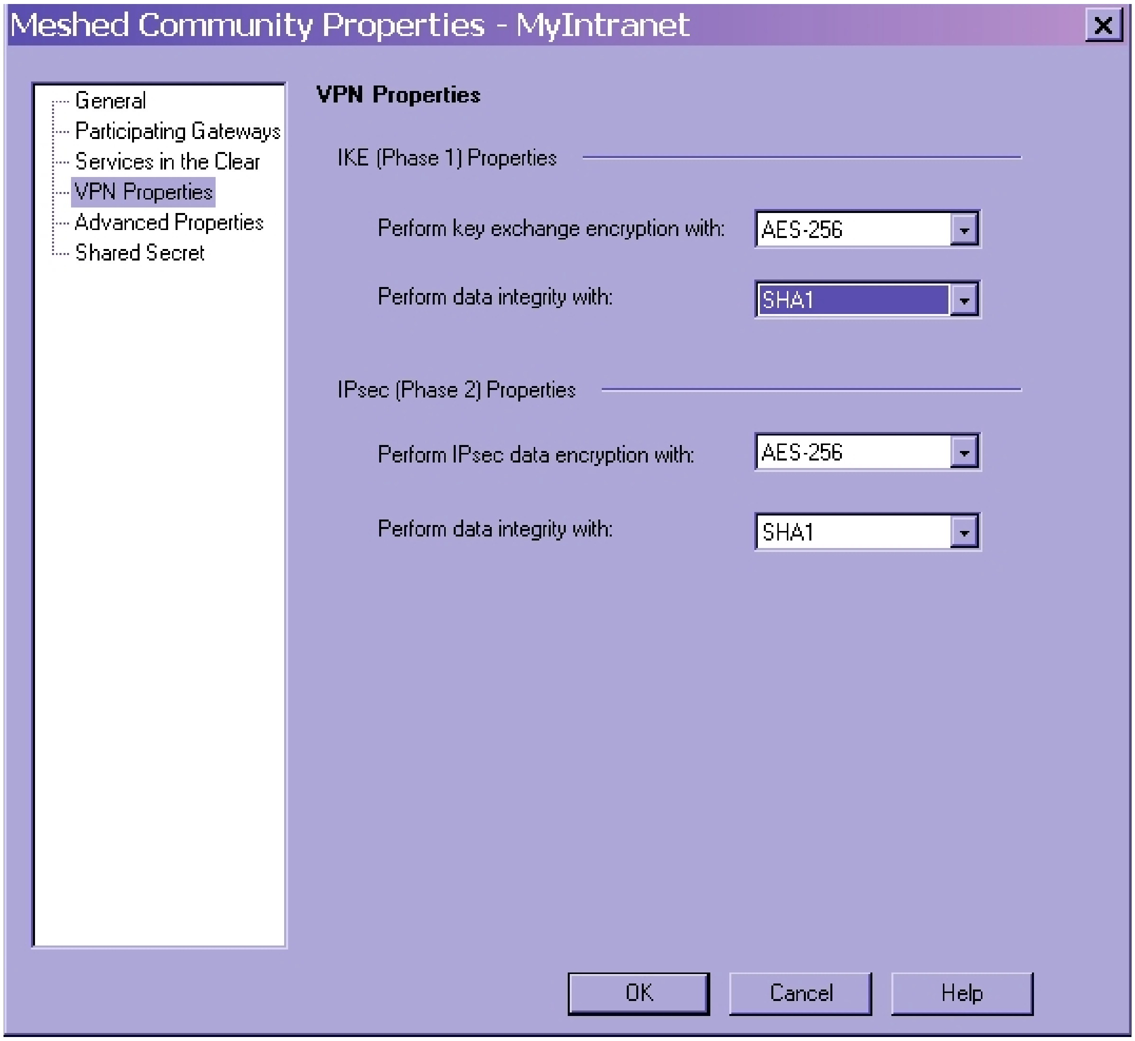
Use Diffie-Hellman groups: Group 2 (1024 bit)

Resolving mechanism

● Enable SecureRemote/SecureClient to calculate statically peer gateway's best interface based on network topology.

○ Enable dynamic interface resolving by SecureRemote/SecureClient peers. (must be defined per gateway)

Figure 7 Only FIPS-Approved Algorithms Can Be Used with IPSec or IKE



Meshed Community Properties - MyIntranet

VPN Properties

IKE (Phase 1) Properties

Perform key exchange encryption with: AES-256

Perform data integrity with: SHA1

IPsec (Phase 2) Properties

Perform IPsec data encryption with: AES-256

Perform data integrity with: SHA1

User Guidance

The User accesses the module VPN functionality as an IPSec client. Although outside the boundary of the module, the User should be careful not to provide authentication information and session keys to other parties.

A Disabled Mechanisms

The following list shows all the access and feature mechanisms that are disabled when the module is in FIPS mode:

- HTTP access
- FTP access
- Telnet access
- TFTP access
- Cluster configuration
- NTP
- Syslog remote logging
- Check Point remote installation daemon
- SSLv3
- Non-FIPS-approved algorithms:
  - Cast
  - DES (40 bits)
  - MD5
  - HMAC MD5
  - Arcfour
  - Twofish
  - Blowfish

B Certificate Numbers

The modules have several independent implementations of the same FIPS-approved algorithm. The following table lists the certificate numbers of the validated FIPS-approved algorithms implemented in Nokia IPSO, the Check Point module, and the Broadcom chips.

FIPS-Approved Algorithm	Certificate Number for the Validated Algorithm Implementation in Nokia IPSO	Certificate Number for the Validated Algorithm Implementation in the Check Point Module	Certificate Number for the Validated Algorithm Implementation in the BCM5802	Certificate Number for the Validated Algorithm Implementation in the BCM5803
AES	N/A	Cert# 88	N/A	N/A
Triple-DES	Cert# 234	Cert# 41 and 80	Cert# 235	Cert# 132
DES	N/A	Cert#110 and 142	Cert# 247	Cert# 183
SHA-1	Cert# 212	Cert# 42 and 69	Cert#210	Cert# 211
DSA	Cert# 99	N/A	N/A	N/A

C Acronyms

The following table contains the acronyms and their meanings that this document uses.

Table 7 Defining Acronyms

Acronym	Meaning
AH	authentication header
AI	Application Intelligence
ANSI	American National Standards Institute
BGP	Border Gateway Protocol
CBC	cipher block chaining
CLI	command-line interface
CMVP	Cryptographic Module Validation Program
CRC	cyclical redundancy check
CSP	critical security parameter
DSA	Digital Signature Standard
DVMRP	Distance Vector Multicast Routing Protocol
EDC	error detection code
EMC	electromagnetic compatibility
EMI	electromagnetic interference
ESP	Encapsulating Security Payload
FCC	Federal Communication Commission
FIPS	Federal Information Processing Standard
FP	feature pack
IGRP	Inter-Gateway Routing Protocol

Table 7 Defining Acronyms

Acronym	Meaning
IKE	Internet Key Exchange
IPSec	IP Security
KAT	known answer test
LED	light emitting diode
MAC	message authentication code
NIST	National Institute of Standards and Technology
OSPF	Open Shortest Path First
PRNG	pseudo random number generator
RAM	random access memory
RIP	Routing Information Protocol
RSA	Rivest Shamir and Adleman
SA	security association
SHA	Secure Hash Algorithm
SIC	secure internal communications
SNMP	Simple Network Management Protocol
SSH	Secure Shell
SSL	Secure Socket Layer
TLS	Transport Layer Security
VPN	virtual private network